TL | Disruption

RISIKEN KLAR IM BLICK

Wer im Gesundheitssektor auf künstliche Intelligenz setzen will, muss hohe datenschutzrechtliche Anforderungen beachten. Welche das sind, wie man sie meistert – und welche neuen, weitreichenden Vorgaben auf EU-Ebene in Sicht sind.

Von Thanos Rammos, Partner bei der Taylor Wessing Partnerschaftsgesellschaft

Der Einsatz künstlicher Intelligenz (KI) hat längst im Gesundheitssektor Einzug gehalten. Schon jetzt findet KI in vielen Bereichen der Gesundheitsvorsorge und Diagnostik Anwendung. Sobald jedoch die Worte „künstliche Intelligenz“, „maschinelles Lernen“ oder „Big Data“ fallen, schrillen auch schon die datenschutzrechtlichen Alarmglocken. Denn der Einsatz von Software mit solcher Funktion birgt einige rechtliche Herausforderungen, die Entscheider im Gesundheitssektor kennen sollten. Bisher wurde der Einsatz von KI unter allgemeinen regulatorischen und datenschutzrechtlichen Aspekten diskutiert. Die Europäische Kommission hat nun einen Vorschlag veröffentlicht, mit dem KI auf europäischer Ebene reguliert und gefördert werden soll. Der Vorschlag enthält bestimmte Anforderungen, die für den Gesundheitssektor weitreichende Konsequenzen haben.

SOFTWAREBASIERTE LÖSUNGEN AUF BASIS VON KI BEZIEHUNGSWEISE MASCHINELLEM LERNEN ERÖFFNEN NEUE MÖGLICHKEITEN IM GESUNDHEITSSEKTOR. VORAUSSETZUNG FÜR DEN ERFOLGREICHEN EINSATZ IST IMMER, EIN HOHES DATENSCHUTZNIVEAU ZU GEWÄHRLEISTEN. DIE EUROPÄISCHE KOMMISSION HAT NUN EINEN VORSCHLAG VERÖFFENTLICHT.

DER EINSATZ VON KI IM GESUNDHEITSSEKTOR

Softwarebasierte Lösungen auf Basis von KI beziehungsweise Maschinellem Lernen eröffnen neue Möglichkeiten im Gesundheitssektor. Ihr Einsatz kann sich von der Diagnostik über die Unterstützung bei Therapieempfehlungen oder der tatsächlichen Behandlung bis hin zu Pflege und Forschung erstrecken. Durch die Möglichkeit, große Datensätze mithilfe eines maschinellen Lernsystems zu analysieren, können neue Erkenntnisse gewonnen werden. Auch die Effizienz lässt sich steigern. Voraussetzung für den erfolgreichen Einsatz ist immer, ein hohes Datenschutzniveau zu gewährleisten. Patientinnen und Patienten, Ärztinnen und Ärzten sowie anderen Stakeholder, wie zum Beispiel Ethik-Kommissionen, sehen KI und Big Data nämlich häufig kritisch. Dies ist verständlich, da zum einen sensible Daten über die Gesundheit verarbeitet werden und zum anderen in Bereiche vorgedrungen wird, die bisher überwiegend menschlicher Beobachtung und Behandlung zugänglich waren.

DATENSCHUTZRECHT MIT ALLGEMEINEN VORGABEN

Das europäische Datenschutzrecht stellt keine spezifischen Anforderungen an KI- oder Big-Data-basierte Softwarelösungen. Vielmehr trifft es allgemeine Vorgaben, die sich jedoch in diesen Bereichen besonders auswirken können. Vor diesem Hintergrund ist es für Entscheider und Anwender aus dem Gesundheitssektor wesentlich, diese Vorgaben im Blick zu haben. Damit sie entsprechende Lösungen ohne Risiken einführen können, bedarf es einer guten Planung. Die Datenschutz-Grundverordnung (DSGVO) ist seit dem 25. Mai 2018 anwendbar. Sie hat das Datenschutzrecht in der EU reformiert und grundsätzlich vereinheitlicht. Die DSGVO erfordert den Aufbau einer umfassenden Compliance-Organisation, auch als Datenschutz-Management-System bekannt. Daneben gilt in Deutschland das angepasste nationale Datenschutzrecht, insbesondere in Form des Bundesdatenschutzgesetzes (BDSG) ergänzend. Neben den allgemeinen datenschutzrechtlichen Vorgaben aus der DSGVO und gegebenenfalls ergänzenden nationalen Sonderregelungen für Krankenhäuser können sich in Deutschland zudem strafrechtliche Risiken im Hinblick auf das Berufsgeheimnis ergeben. Um insoweit risikofrei zu sein, sollten entweder einschlägige Entbindungen von der Schweigepflicht in den Einwilligungserklärungen berücksichtigt werden oder aber in entsprechenden Vereinbarungen mit den Anbietern einer KI-basierten Softwarelösung entsprechende Vorkehrungen getroffen werden. Krankenhäuser mit öffentlich-rechtlicher Trägerschaft müssen andere Rahmenbedingungen als privatrechtlich organisierte Kliniken beachten. Das jeweilige Landesrecht sieht für sie unter Umständen bestimmte Einschränkungen vor. Sind Krankhäuser kirchlich organisiert, sind kirchliche Datenschutzvorschriften einzuhalten. Die folgenden Vorgaben aus der DSGVO sind für KI und Big Data im Gesundheitssektor besonders relevant.

ZWECKBINDUNGS-GRUNDSATZ

Die Zweckbindung ist ein wesentlicher datenschutzrechtlicher Grundsatz. Sie verlangt, dass für einen bestimmten Zweck erhobene Daten nur für genau diesen Zweck verwendet werden und ihre Weiterverarbeitung mit diesem vereinbar ist. Das muss bereits berücksichtigt werden, wenn die Gesundheitsdaten erhoben werden, die später durch maschinelles Lernen oder eine Big-Data-Anwendung analysiert werden sollen. Diese Anforderung einer strengen Zweckbindung ist jedoch dann gelockert, wenn Daten für wissenschaftliche Forschungszwecke weiterverarbeitet werden, die im öffentlichen Interesse liegen. Dies kann im Gesundheitssektor also Vorteile bringen.

GRUNDSATZ DER DATENMINIMIERUNG

Ein weiteres allgemeines Prinzip des Datenschutzrechts ist die sogenannte Datenminimierung. Danach sind immer so wenig wie möglich Daten zu verarbeiten. Sprich: Nur so viele, wie zur Erreichung des Zwecks notwendig sind. Der Grundsatz kann den Einsatz von KI erschweren. Denn meist sind diese Lösungen auf die Auswertung besonders umfangreicher Datenmengen angewiesen. Keine Anwendung findet das Datenschutzrecht allerdings, wenn Informationen anonymisiert worden sind. Nach Möglichkeit sollten daher Daten nur in anonymisierter Form für die KI genutzt werden.

RECHTMÄSSIGKEIT DER DATENVERARBEITUNG

Bei dem Einsatz von KI im Gesundheitssektor wird es häufig um die Verarbeitung besonders sensibler Daten gehen. Dazu zählen alle Informationen über den Gesundheitszustand, aber natürlich auch genetische und biometrische Daten. Das Datenschutzrecht stellt an die Verarbeitung solcher Daten besonders strenge Anforderungen. Es bedarf daher entweder einer besonderen gesetzlichen Erlaubnis oder der Einwilligung der Patientinnen und Patienten, die sich auf die Verarbeitung von Gesundheitsdaten bezieht. Zu den Erlaubnisvorschriften, die eine entsprechende Verarbeitung gestatten, gehören die medizinische Diagnostik, Versorgung oder Behandlung oder die Verwaltung von Systemen und Diensten im Gesundheitssektor. Die Aufsichtsbehörden legen diese Begriffe grundsätzlich eng aus.

Unter engen Voraussetzungen ist die Datenverarbeitung auch für wissenschaftliche Forschungszwecke erlaubt. Im Einzelfall dürfen Gesundheitsdaten daher zu klinischen Studien verarbeitet werden, wenn diese im öffentlichen Interesse liegen. Aufgrund der engen Voraussetzungen empfiehlt es sich derzeit meist noch, den Einsatz von Big

→

Thanos Rammos, Partner bei der Taylor Wessing Partnerschaftsgesellschaft

Data oder KI-basierender Software auf eine Einwilligung der Patientinnen und Patienten zu stützen.

EINWILLIGUNGSGEBOT

Für den Einsatz von KI sollten Einwilligungen von Patientinnen und Patienten mit großer Umsicht eingeholt werden. Eine Einwilligung ist nur wirksam, wenn sie informiert erfolgt. Um eine wirksame Einwilligung einzuholen, muss die entsprechende Erklärung so entworfen sein, dass die notwendige Transparenz gewährleistet ist. Dem Betroffenen sind nicht nur der Zweck sowie die Art und Weise der Verarbeitung seiner Daten, sondern unter anderem auch deren Empfänger mitzuteilen. Bei Big-Data-Anwendungen stellt dies eine Herausforderung dar, weil sich die Zwecke häufig im Voraus nicht vollends bestimmen lassen. Bei KI-Lösungen soll der Algorithmus häufig aufbauend auf verschiedenen Datenquellen lernen. Patientinnen und Patienten hierbei transparent darzulegen, was mit ihren Daten genau passiert, ist nicht unmöglich, bedarf aber einer bedachten Formulierung.

Darüber hinaus muss die Einwilligung freiwillig erteilt werden. Zudem muss die Einwilligung ausdrücklich erteilt werden und kann nicht etwa aus einem schlüssigen Verhalten gefolgert werden. Bei mehreren Einwilligungen, zum Beispiel im Rahmen von klinischen Studien, bietet es sich an, diese modular zu gestalten. Das heißt: Es empfiehlt sich, mit unterschiedlichen Kästen oder Checkboxen zu arbeiten.

WIDERRUF DER EINWILLIGUNG

Eine weitere Herausforderung besteht darin, dass Patientinnen und Patienten stets von Gesetzes wegen die Möglichkeit haben müssen, ihre Einwilligung zu widerrufen. Aufgrund dessen ist es besonders bei Algorithmen, die auf der Basis von vorhandenen Daten lernen oder Vorhersagen treffen sollen, schwierig, wenn dieser Berechnung die Grundlage entzogen wird. Zu beachten ist jedoch, dass der Widerruf nur Wirkung für die Zukunft hat. Ferner gilt ein Widerruf nicht bei Informationen, die anonymisiert worden sind. Wer eine entsprechende Software einführen und anwenden will, sollte die Datenbasis daher mit Augenmaß und diesen Überlegungen im Hinterkopf erstellen.

RECHT AUF LÖSCHUNG

Ein wichtiges und im Zusammenhang mit KI und Big Data besonders relevantes Recht ist die Löschung. Sie ist auch als „Recht auf Vergessenwerden“ bekannt. Das Recht greift bei jedem personenbezogenen Datum, sobald es nicht mehr für die jeweiligen Zwecke erforderlich ist und keinen besonderen Aufbewahrungspflichten unterliegt. Bei Big-Data- und KI-basierten Lösungen muss sichergestellt sein, dass Patientinnen und Patienten auch bei solchen Anwendungen ihr Löschungsrecht ausüben können, ohne dass diese zugleich „leer laufen“, weil die Grundlage der Datenanalyse gelöscht wird. Auch mit Blick auf dieses Recht ist es also sehr wichtig, die Datenbasis möglichst frühzeitig zu anonymisieren.

ÄRZTLICHES BERUFSGEHEIMNIS

Ein weiterer Aspekt ist der Umgang mit der ärztlichen Schweigepflicht. Bis vor Kurzem hat das strafrechtlich geschützte Berufsgeheimnis den Einsatz solcher Softwarelösungen erschwert, die Daten von Patientinnen und Patienten an Dritte übermitteln konnten. Durch eine Anpassung der strafrechtlichen Vorschriften können Ärztinnen und Ärzte sowie Krankenhäuser nun in erweitertem Umfang auf externe Dienstleister zurückgreifen. Dies wirkt sich auch auf KI- und Big-Data-Anwendungen positiv aus. Denn externe Anbieter haben regelmäßig Zugriff auf die Daten, wie etwa bei einer Wartung. Die strafrechtlichen Neuerungen haben jedoch keine Auswirkungen auf die datenschutzrechtliche Zulässigkeit der Inanspruchnahme von Dienstleistern. Wie bisher müssen die Voraussetzungen einer sogenannten Vereinbarung zur Auftragsverarbeitung beachtet werden. Darin müssen die Vorgaben zur Wahrung des ärztlichen Berufsgeheimnisses enthalten sein.

EU-VORSCHLAG FÜR EINE KI-VERORDNUNG

Neue Anforderungen an den Einsatz von KI im Gesundheitssektor könnten sich zudem aus den jüngsten Vorschlägen auf EU-Ebene ergeben. Dabei handelt es sich um eine Verordnung für Design, Verwendung und Entwicklung von KI. Die Europäische Kommission hat den Vorschlag im April 2021 veröffentlicht. Er geht auf das sogenannte Weißbuch der EU zurück, welches vor circa zwei Jahren erstellt wurde. Ziel ist es, Europa zu einem globalen Zentrum für vertrauenswürdige KI zu machen. Die Kommission folgt in ihrem Entwurf einem sogenannten risikobasierten Ansatz. Das bedeutet: Je nach Gefährdungspotential der KI für zentrale Rechtsgüter von EU-Bürgern, wie etwa Gesundheit, Sicherheit und Grundrechte, sollen unterschiedliche Anforderungen an die Entwicklung und die Nutzung von KI gelten. Dabei werden die Anwendungen in folgende vier Kategorien eingeteilt:

i) verbotene Anwendungen mit inakzeptablem Risiko, ii) Hochrisiko-Anwendungen, iii) Anwendungen mit besonderen Merkmalen und iv) sonstige Anwendungen mit minimalem Risiko.

ANFORDERUNGEN JE NACH RISIKOKATEGORIE

Zur ersten Kategorie der inakzeptablen Risiken gehören besonders schädliche Anwendungen von KI. Dazu zählen Lösungen, die eine Bedrohung für die Sicherheit, die Lebensgrundlagen und die Rechte der Bürgerinnen und Bürger darstellen. Als Beispiele werden KI-Systeme genannt, die der Manipulation menschlichen Verhaltens dienen, wie etwa „Social Scoring“-Systeme von Regierungen.

Im Bereich der Hochrisiko-Anwendungen unterliegt der Einsatz von KI strengen Anforderungen. Erfasst werden insbesondere KI-Anwendungen in gefahrgeneigten Bereichen wie dem Straßenverkehr, der Luftfahrt, der Strafverfolgung aber vor allem auch der Medizin. Solche KI muss vor dem Inverkehrbringen eine sogenannte „Konformitätsbewertung“ durchlaufen. Dies soll nachweisen, dass sie die verbindlichen Anforderungen an vertrauenswürdige KI erfüllt. Hierzu zählen beispielsweise Datenqualität, Dokumentation und Nachvollziehbarkeit, Transparenz, menschliche Aufsicht, Genauigkeit und Robustheit.

In die dritte Kategorie fallen KI-Anwendungen, die mit Menschen interagieren. Dazu zählen beispielsweise Chatbots oder Anwendungen, die Inhalte generieren beziehungsweise manipulieren können. Bei solchen Anwendungen soll künftig kenntlich gemacht werden, dass hierbei KI zum Einsatz kommt.

KI mit minimalem Risiko soll von der Verordnung nicht erfasst sein und weiterhin entwickelt und verwendet werden dürfen. Darunter fällt die Mehrheit der KI-Anwendung, wie beispielsweise KI-fähige Videospiele oder Spamfilter,

Je nach Anwendung kann die Entwicklung und der Einsatz von KI im medizinischen Bereich also zu verschiedenen der vier Kategorien gehören. Es wird im Einzelfall zu prüfen sein, welche zusätzlichen Anforderungen an die Anwendung gestellt werden.

FAZIT

Um das Potenzial von KI und Big Data im Gesundheitswesen auszuschöpfen, müssen Entscheiderinnen und Entscheider datenschutzrechtliche und sonstige regulatorische Herausforderungen frühzeitig erkennen und schon bei der Einführung berücksichtigen. Es ist zwingend, dass die Daten nur für den Zweck genutzt werden, für den sie erhoben wurden. Sie sollten möglichst nur in anonymisierter Form eingesetzt werden. Ein besonderes Augenmerk sollte zudem darauf liegen, wie die Einwilligungen bei Patientinnen und Patienten eingeholt werden. Mit Blick auf den Vorschlag der EU-Kommission für die KI-Verordnung bleibt abzuwarten, inwieweit er umgesetzt wird – und welche weiteren Anforderungen hiermit für den Einsatz künstlicher Intelligenz im Gesundheitsbereich einhergehen.

WIE DIE EU-KOMMISSION KI-RISIKEN EINTEILT

Risikokategorie	Anforderung
KI mit inakzeptablem Risiko z.B. „Social Scoring" durch Regierungen	Einsatz verboten
KI mit hohem Risiko z.B. kritische Infrastrukturen, medizinische Geräte	Konformitätsbewertung vor Inverkehrbringen
KI mit bestimmten Merkmalen (Interaktion mit Menschen) z.B. Chatbots	Transparenz-/Offenlegungspflicht
KI mit minimalem Risiko z.B. KI-fähige Videospiele oder Spamfilter	Entwicklung/Einsatz unterfällt nicht der Verordnung und ist weiter möglich

Quelle: Eigene Darstellung